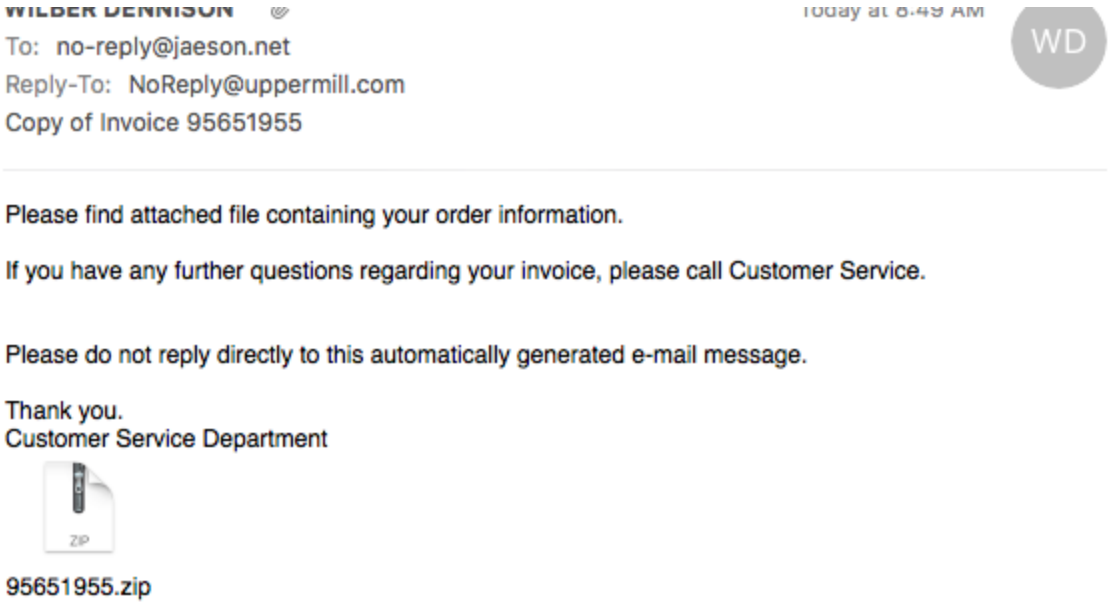
Player 1 Limps Back Into the Ring - Hello again, Locky!

blog.talosintelligence.com/2017/06/necurs-locky-campaign.html


WILBER DENNISON Today at 8:49 AM

To: no-reply@jaeson.net

Reply-To: NoReply@uppermill.com

Copy of Invoice 95651955

WD

Please find attached file containing your order information.

If you have any further questions regarding your invoice, please call Customer Service.

Please do not reply directly to this automatically generated e-mail message.

Thank you.
Customer Service Department

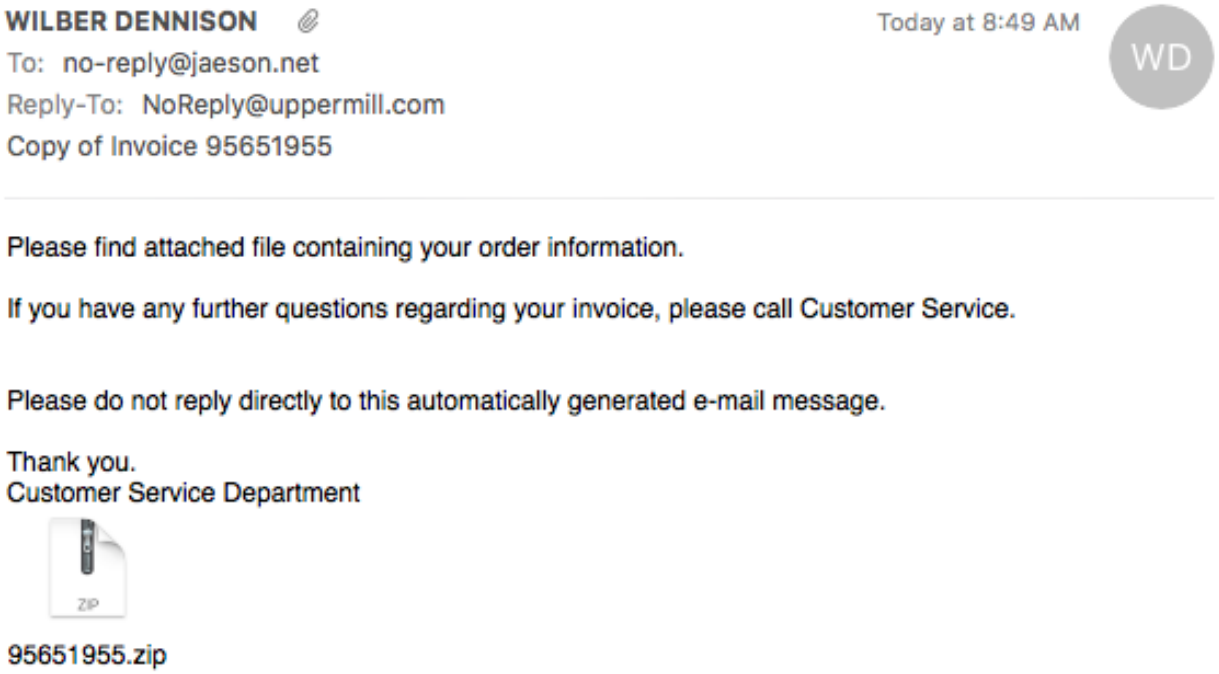
ZIP

95651955.zip

Back in May, the Necurs spam botnet jettisoned Locky ransomware in favor of the new Jaff ransomware variant. However, earlier this month Kaspersky discovered a vulnerability within Jaff which allowed them to create a decryptor. This turn of events seems to have caused the miscreants behind Necurs to scramble to distribute a different ransomware payload. Falling back on their old tricks, they have selected to re-distribute Locky ransomware. The malware is being transmitted via email using an .exe file encapsulated within two compressed .zip archives.

The Spam Campaign

The spam that is distributing this ransomware campaign is not significantly different from other ransomware spam campaigns that we have seen from Necurs. Ransomware-oriented spam campaigns from Necurs typically involve order confirmations, payment receipts, business documents, and so on -- all with the common goal of social engineering victims into opening the attachment. The messages Talos observed in this particular campaign are disguised as fake invoices.



An example spam message propagating Locky ransomware

The volume of Locky spam Necurs has sent since the start of this particular campaign is notable. In the first hour of this campaign, Talos observed that Locky spam accounted for up to 7.2% of email volume on one of our systems. While the campaign has since decreased in the number of messages being sent per minute, Necurs is still actively sending messages containing Locky, though only in small quantities.

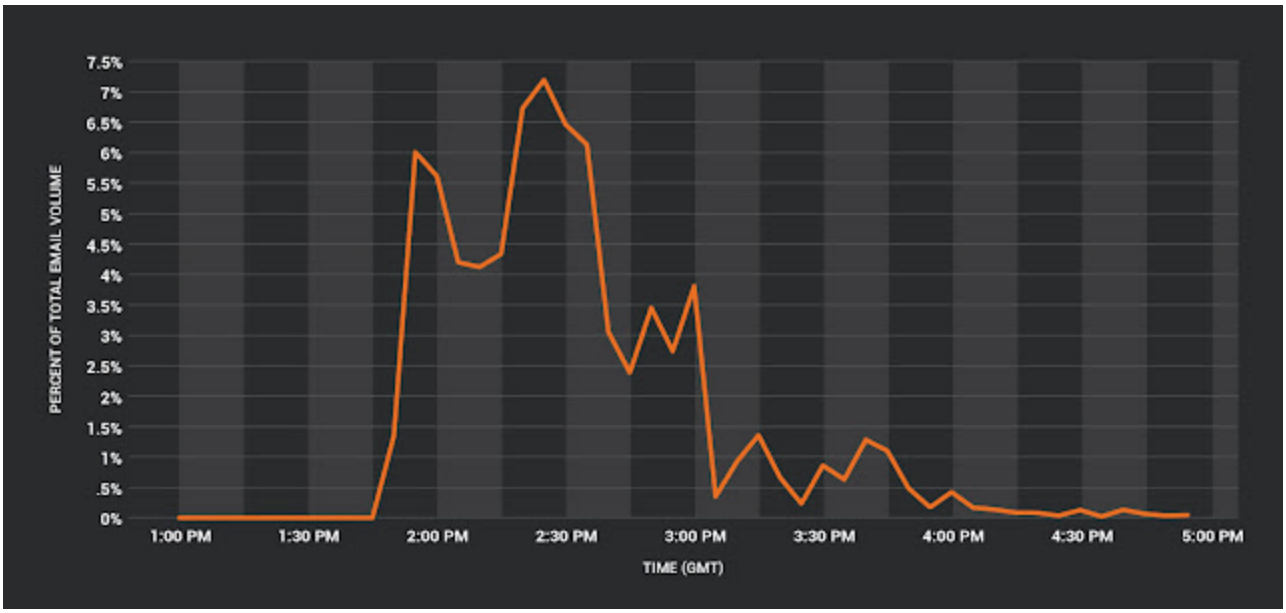


Chart illustrating the volume of Locky spam as a percent of total email volume one of our systems observed.

Locky's Metamorphosis

Although they are using the same affiliate ID, for this particular round of Locky, the attackers have altered their ransomware. We were unable to get the ransomware to encrypt data on any systems running an operating system more recent than Windows XP. Upon further investigation, we determined that on systems running Windows 7 or later with Data Execution Prevention (DEP) would cause the unpacker to fail. Our analysis suggests that Locky has now added anti-debugging protection to their configuration. Instead of unpacking the configuration, when a debugger is detected their config pointer is directed at kernel32!AllocConsole, frustrating any attempts at analysis. In response to this new anti-analysis technique, Talos has updated LockyDump so that it is able to extract the configuration information from this latest iteration.

```
eax=00000020 ebx=00000047 ecx=0018cb74 edx=00000baa esi=0004c923 edi=00000bab
eip=0018cb74 esp=0018c064 ebp=000281bd iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
0018cb74 e80d020000      call    0018cd86
0:000> !address 0018cb74

Mapping file section regions...
Mapping module regions...
Mapping PEB regions...
Mapping TEB and stack regions...
Mapping heap regions...
Mapping page heap regions...
Mapping other regions...
Mapping stack trace database regions...
Mapping activation context regions...

Usage:                  Stack
Base Address:           0018a000
End Address:            00190000
Region Size:            00006000 (  24.000 kB)
State:                  00001000          MEM_COMMIT
Protect:                00000004          PAGE_READWRITE
Type:                   00020000          MEM_PRIVATE
Allocation Base:        00090000
Allocation Protect:     00000004          PAGE_READWRITE
More info:              ~0k

Content source: 1 (target), length: 48c
```

Locky's unpacker crashes when trying to execute stack memory on systems more recent than Windows XP.

Another notable aspect of this latest campaign was the C2 URL structure. Adversaries behind this latest Locky campaign have reused the /checkupdate path as part of the URL structure -- the same URL structure found in previous Locky campaigns. This is perhaps

another indication that adversaries were hasty in their developing and distributing this campaign.

Threat Grid sandbox run illustrating Locky C2 communication

Conclusion

This updated version of Locky appears to have been hastily deployed, and as a result it has not affected users running Windows operating systems other than Windows XP. The attackers behind this ransomware are likely already aware of this, so we can expect a fixed version of Locky to appear in a future round of Necurs' ransomware spam.

Despite sounding like a broken record, we at Talos feel it's our duty to re-iterate that it's always risky clicking on links or opening attachments in strange email messages. Users that fail to heed this advice can easily become ransomware victims, and if the subsequent ransom is paid, the monies will no doubt fund another round of attacks. As always, organizations are encouraged to make regular backups of their data, practice restoring said data, and store your backups offline far out of the reach of potential criminals.

Coverage

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS, WSA, and Umbrella can help identify hosts that have been compromised by Locky by detecting outbound C2 traffic.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as NGFW, NGIPS, and Meraki MX with Advanced Security can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Stealthwatch detects network scanning activity, network propagation, and connections to CnC infrastructures, correlating this activity to alert administrators.

IOCs

SHA256

- 49184047c840287909cf0e6a5e00273c6d60da1750655ad66e219426b3cf9cd8
- 3285c3f37aa192a173f62fee82f7a966a6df6e5db4642d63a6784f39a63012b6

File Extension for Files Encrypted by Locky

.loptr

Hard-coded Locky C2 URL

hxxp://185.115.140[.]170/checkupdate

Locky DGA C2s (20th/21st June - DGA seed 65123)

- hxxp://emtsgdqsik[.]pl/checkupdate
- hxxp://tqathwvfaqfisj[.]pl/checkupdate
- hxxp://dqutujymgc[.]info/checkupdate
- hxxp://ddgtdcgoysuq[.]ru/checkupdate
- hxxp://lrsjplrlaceugxw[.]work/checkupdate
- hxxp://cstfxgujaf[.]biz/checkupdate
- hxxp://gcbdwbtshl[.]xyz/checkupdate
- hxxp://wxcjqfevrkosp[.]biz/checkupdate
- hxxp://hllfhiqwneuwwx[.]biz/checkupdate
- hxxp://agnfmqvhomsa[.]work/checkupdate
- hxxp://ythjvjhtgsfgesd[.]biz/checkupdate
- hxxp://kabssqyef[.]info/checkupdate